ASSET MANAGEMENT TOWARDS ISO/IEC 27001:2005 ACCREDITATION OF AN INFORMATION SECURITY MANAGEMENT SYSTEM

Daniel COSTIN
Constantin MILITARU
Politehnica University of Bucharest, Romania

ABSTRACT

Currently, ISO/IEC 27001:2005 is the formal specification standard for Information Security Management System (ISMS), against which organizations may seek certification. This International Standard adopts a process approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organization's ISMS. The "Asset management" main clause deals with information asset management, including classification and acceptable use. The objective of this control is to achieve and maintain appropriate protection of organization's information assets. In today's environment, organizations depend on sharing information and information classification is a key concept in the structuring and development of an effective ISMS: the classification given to a particular information asset can determine how it is to be protected, who is to have access to it, what networks it can run on etc.

The ISO/IEC 27001:2005 Standard specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving formalized information security management systems (ISMS) within the context of the organization's overall business risks. It specifies requirements for the implementation of security controls customized to the needs of individual organizations or parts thereof. This International Standard is universal for all types of organizations. Benefits of pursuing certification to ISO/IEC 27001:2005 include:

- Certification allows organizations to mitigate the impact of information security breaches when they do occur;
- Certification allows organizations to demonstrate due diligence and due care to shareholders, customers and business partners, through strategic thinking;
- Certification allows organizations to demonstrate proactive compliance to legal, regulatory and contractual requirements;
- Certification provides independent third-party validation of an organization‟s ISMS;
- ISO/IEC 27001 is the most comprehensive information security management certification that is internationally accepted.

The ISO/IEC 27001:2005 Standard contains 11 security control clauses, illustrated in figure 1. Each clause contains a number of main security categories. Depending on the circumstances, all clauses could be important; each organization applying this standard should identify applicable clauses to the individual business processes.

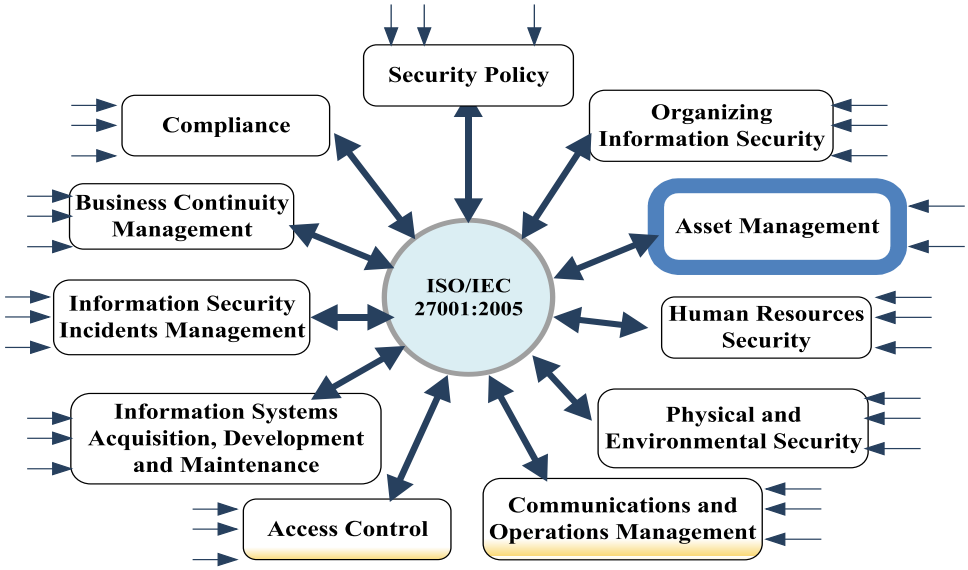

Figure 1 The 11 security control clauses of the ISO/IEC 27001:2005 Standard

Control A.7 of the standard deals with asset management, including classification and acceptable use. The objective of this control is „to achieve and maintain appropriate protection of organizational assets".

The ISO/IEC 27001:2005 standard defines the term asset as "anything that has value to an organization". Assets can range from data files to physical assets, such as removable media; however, the ISO definition allows an organization to classify items as assets from a broader spectrum. Intangibles, such as reputation of the organization, general utilities, and the skill sets of a workforce can all be classified as assets.

"**Responsibility for assets**" is the first of two main security categories listed under the Asset management clause. According to the ISO/IEC 27001:2005, the overall objective of asset responsibility is to achieve and maintain adequate protection of assets. To achieve this objective, the 17799 standard has listed three controls: Inventory of Assets, Ownership of assets and acceptable use of assets..

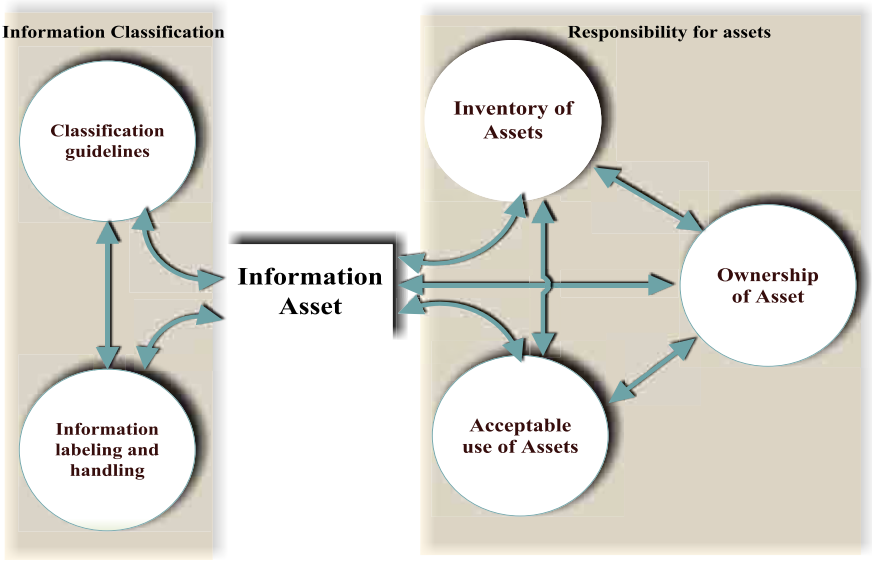

Figure 2 "Asset management" clause of ISO/IEC 27001:2005 standard

The "control specifically requires the organization to identify all important information assets and to draw up and maintain an inventory of them".

The types of assets that ISO/IEC 27001:2005 identified as needing to be inventoried include the following:

- Information assets: data in any format. Files and copies of plans, system documentation, original user manuals, original training material, operational or other support procedures, continuity plans and other fall-back arrangements, archived information, personal data, financial and accounting information.
- Software assets: application software, operating system software, development tools and utilities, e-learning assets, network tools and utilities.
- Physical assets: computer equipment (including workstations, notebooks, PDAs, monitors, modems, scanning machines, printers), communications equipment (routers, cell phones, phone systems, fax machines, answering machines, voice conferencing units, etc), magnetic media (CD ROMs, tapes, disks, memory sticks), other technical equipment (power supplies, air conditioning units), furniture, other equipment.
- Services: general utilities, gas, electricity, water.
- People: their qualifications, skills and experience.
- Intangible assets such as reputation and brand.

The inventory should have a nominated owner and the procedures for maintaining it and, in particular, for accessing it in a disaster recovery situation should be clearly documented.

The importance of an asset can be measured by its business value and security classification or label. Assets value must be set on the basis of the impact that compromises of their availability, confidentiality and integrity may have on the organization.

The asset inventory should identify each asset, describe it or provide such other identification that the asset can be physically identified and full details (including maker, model, generic type, serial number, date of acquisition and any other numbers) included in the inventory, its current location and any other information necessary for disaster recovery. The nominated owner of the asset should be shown on the schedule, as should its security classification. The inventory should be updated regularly.

Control "**Ownership of assets**" says that all information assets should have a nominated owner and should be accounted for. The "owner" is the person, or function, that has responsibility for the asset; the "owner" has no property rights to the asset. This control requires the organization to maintain, among the ISMS documentation, a schedule that shows all the information assets of the organization. This person"s responsibility for the asset should be set out and described in a formal document (signed). The document should describe the asset for which the person is responsible and its location. It should describe the security controls (including the security classification and access restrictions) that are required for the asset and set out the owner"s responsibility for maintaining (and periodically reviewing) them. A copy should be retained along with the asset schedule.

The owner may be allowed to delegate responsibility for implementing or maintaining controls to staff directly responsible but should not be allowed to delegate accountability. This should rest squarely and clearly with the nominated owner.

It is much more difficult to determine the owners of the intangible information assets. It is important to get this right because the owner will have specific responsibilities.

In terms of new documents, the organization could simply adopt the policy that the originator of an information asset will be defined as its owner. This would cover, for instance, business plans, forecasts, client letters and project plans, etc.

There are other information assets, however, whose use through the organization will be widespread and whose origination is the result of a strategic or group decision. The only practical approach to these assets is for the organization, at the time that it decides to create it, to decide who will be the owner and to write this into the person"s job description. Usually, the owner should be the person who uses it most, or has most control over it.

Control "**Acceptable use of assets**" of the standard requires organizations to document and implement rules for the acceptable use of information assets, systems and services. These rules should apply to employees, contractors and third parties. Policies for acceptable use should be drawn up to include e-mail and internet usage, mobile devices (telephones, PDAs and laptops) and usage of information systems beyond the organization"s fixed perimeter.

The "information classification" category of ISO/IEC 27001 standard ensures that information receives an appropriate level of protection.

Control "**Classification guidelines**" of the standard specifies that an organization must have a procedure for classifying information to ensure that its information assets receive an appropriate level of protection.

The standard simply requires that classifications should be suited to business needs to restrict and to share information. It is important to note that sharing is as important as is restricting; it is possible to draw up a set of guidelines that are too restrictive for the business but that are therefore regularly breached.

In today"s environment organizations depend on sharing information; it is essential that information is classified in such a way that this can be done consistently and appropriately. Whatever classification scheme is adopted by the organization should be extended to cover the level at which users can access data in the system (read only, write and delete).

Information classification is a key concept in the structuring and development of effective ISMS. The classification given to a particular information asset can determine how it is to be protected; who is to have access to it, what networks it can run on, etc.

The benefits of adopting a consistent procedure for the organization:

- reduce the risk of damage to its reputation, profitability or interests due to loss of sensitive information;
- increase confidence in trading and funding partnership;
- simplify the exchange of sensitive information with third parties, while ensuring that risks are appropriately managed.

Classified information is marked so that both originator and recipient know how to apply appropriate security to it. The classification is based on the likely impact on the organization if the information is leaked or disclosed to the wrong third-party organizations or people. Any system the organization adopts must be clear, clearly documented and clearly understood by everyone who uses it.

The simplest approach has only three levels of classification: Confidential (ex. be restricted to a specific list of people), Restricted and Private (should cover everything that has value but that does not need to fall within either of the other categories).

The organization also needs to consider how it will appropriately classify third-party-sensitive documents that it receives and that it will be responsible for protecting.

The asset owner is responsible to assign and enforce appropriate classification to all information and information technology to protect these assets accordingly.

Control "**Information labeling and handling**" of the standard requires the organization to implement a set of procedures for information labeling and handling that reflects the information classification scheme adopted. These procedures need to cover all formats of information asset, both physical and electronic. There should be procedures for the following types of information

processing activity:

- acquisition of information;
- copying (electronically, by hand and through other means);
- storage, both electronic and in hard copy;
- transmission by fax, post, e-mail and infrared synchronization;
- transmission by spoken word, including mobile phone, voicemail and answering machines;
- logging of security events;
- destruction - when no longer required.

Specific consideration needs to be given for labeling of electronic assets in a way that is rigorous and reliable.

Managing and securing an organization"s assets can be a difficult task. The "asset management" main clause of ISO/IEC 27001 standard establishes the blueprint to identify the rules of acceptable use and the rules for protection: what assets to protect, who protects them and how much protection is adequate.

To account for the assets that require protection, the standard specifies the requirement to designate who owns assets. Designated owners become responsible for protecting information and technology assets and to maintain the way assets are protected.

The standard sets the foundation for a system that classifies information to identify different security levels, to specify how much protection is expected and how information should be handled at each level. Not all the information requires the same level of protection because only some information is sensitive or confidential. Developing an inventory of assets, defining owners of assets, establishing acceptable use policies and classifying and labeling information are all controls that can be implemented to ensure information and assets receive appropriate protection.

Bibliography

1. ISO/IEC 27001:2005 Information technology - Security techniques - Information Security Management Systems - Requirements
2. ISO/IEC 27002:2005 Information technology - Security techniques - Code of practice for information security management
3. Bidgoli, Hossein: *Handbook of Information Security*, Volume 3, Published by John Wiley & Sons, Inc., Hoboken, New Jersey. 2006, ISBN-13: 978-0-471-64832-1
4. Coyne, Edward J.; Davis, John: *Role Engineering for Enterprise Security Management*. Artech House, Inc., 2008, ISBN: 978-1-59693-218-0
5. Khadraoui, Djamel; Francine, Herrmann: *Advances in Enterprise Information Technology Security Information*, Science Reference (IGI Global), New York 2007, ISBN 978-1-59904-090-5
6. Subramanian, Ramesh: *Computer Security, Privacy and Politics: Current Issues, Challenges and Solutions*. IRM Press, New York, 2008 ISBN: 978-1-59904-804-8